THE 1996 UNITED NATIONS' COMMISSION ON INTERNATIONAL TRADE LAW MODEL LAW ON ELECTRONIC COMMERCE AND GUIDE TO ENACTMENT

*Houston Putnam Lowry**

The United Nations' Commission on International Trade Law (hereinafter UNCITRAL) was formed by the United Nations General Assembly in 1966.[1] UNCITRAL has undertaken many projects since that time.[2] The projects have dealt with the important issues of international commerce, including arbitration, the sale of goods,[3] bills and notes,[4] and letters of credit.[5]

UNCITRAL even prepared a resolution on the legal value of computer records in 1985.[6] UNCITRAL recognized early that computers have a profound influence on the day-to-day conduct of business. Something had to be done to harmonize domestic laws and to eliminate barriers to take advantage of computers, a technology that knows no boundaries. The law must keep up with technology if it is to remain relevant. UNCITRAL's

---

* Mr. Lowry is a member of Brown & Welsh P.C., Meriden, Connecticut, and the Chair of the International Commercial Committee of the American Branch of the International Law Association.

1. G.A. Res. 2205, U.N. GOAR, 21st Sess., Annex II, at 41, 42, U.N. Doc A/6394/Add. 1/Add.2 (1966).

2. Such as the 1958 New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards <http://www.un.or.at/uncitral/english/texts/arbconc/index.htm>; 1974 Convention of the Limitation Period in the Sale of Goods, as amended in 1980 <http://www.un.or.at/uncitral/english/texts/sales/limitcon.htm#TOP>;1976 UNCITRAL Arbitration Rules <http://www.un.or.at/uncitral/english/texts/arbconc/arbitrul.htm>; 1980 UNCITRAL Convention on Contracts for the International Sale of Goods, commonly called the 1980 Vienna Convention<http://www.un.or.at/uncitral/english/texts/sales/salescon.htm#TOP>; 1985 UNCITRAL Model Law on International Commercial Arbitration <http://www.un.or.at/uncitral/english/texts/arbconc/ml-arb.htm>; 1988 UNCITRAL Bills and Notes Convention (http://www.un.or.at/uncitral/english/texts/payments/bilnote.htm#TOP); 1996 United Nations Convention on Independent Guarantees and Stand-by Letters of Credit (http://www.un.or.at/uncitral/english/texts/payments/guarant.htm) and 1996 UNCITRAL Arbitration Notes <http://www.un.or.at/uncitral/english/texts/arbconc/arbnotes.htm>.

3. *See* U.C.C. art. 2 (1997).

4 *Id.* art. 3 (1997).

5. *Id.* art. 5 (1997).

6. <http://www.un.or.at/uncitral/english/texts/electcom/legval.htm>.

solution, the Model Law on Electronic Commerce (hereinafter Law),[7] was approved by the General Assembly on December 16, 1996. UNCITRAL also prepared a Guide to Enactment of the Law. While the Law has been enacted only in Singapore, it has been introduced in a number of jurisdictions.[8]

The Law governs a number of technologies. First of all, it governs faxes.[9] There has been a lively debate for a number of years as to whether a faxed document was a legally binding document. This law puts that question to rest, but for a novel reason. Businesses use faxes on a day-to-day basis. It is getting increasingly difficult to tell where the fax ends and the electronic technology begins. Should the way a person sends a data message[10] from a computer (by a fax instead of an e-mail) determine the legal effect of the document?[11] Should the fact that a person sends a fax from a computer instead of a fax machine change the legal effect of the fax (particularly since the recipient cannot tell which method was used)? Should how the recipient elects to store a fax (on a piece of paper or in a computer) determine the legal effect of a document (particularly since this fact cannot be determined by the sender)? Logic prevailed because all three questions were answered in the negative.

When UNCITRAL's project began, the focus was on electronic data interchange (hereinafter EDI).[12] EDI is a structured system. The sender agrees to send data in a certain format. The recipient agrees to accept data in a certain format. By the time the project was several years old, the drafters realized the EDI concept was as outmoded as trying to conceive of data messages in columns punched on the proverbial IBM computer card. EDI technology was certainly used in the past. Some organizations were still using the technology when the drafting started. Everyone agreed they hoped to shift to a different technology in the near future, even if only to a web based technology. Therefore, the scope of the Law was expanded to include all kinds of data messages and not just EDI.[13]

The drafters also recognized they could not predict where technology was going. While the new topic is a Java based world wide web technology today, no one could say what will be the new topic tomorrow.

---

7. UNCINTRL Model Law on Electronic Commerce with Guide to Enactment http://www.un.or.at/uncitral/english/texts/electcom/ml-ec.htm [herinafter Law J.].

8. *See,* H.B. 5470 introduced in the 1998 Session of the Connecticut General Assembly, for an example.

9. Law, *supra* note 7, art. 2(a).

10. *Id.* art. 2(a).

11. Particularly since the creation of fax modems.

12. Law, *supra* note 7, art. 2(b).

13. *Data message* means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy.

The Law was designed to be technology neutral. It will not have to be re-drafted as new technologies come into use.

The very concept of a model law requires it to be interpreted in a consistent manner in different jurisdictions. Precedent from other jurisdictions must be considered, as well as the *traveux preparatoire* from UNCITRAL. This concept was included in Article 3 of the Law.[14] As a result, UNCITRAL will begin reporting cases under the Law as part of their CLOUT (Case Law on UNCITRAL Texts)[15] project.

In keeping with its stated position of providing flexibility with the commercial area, the United States took a strong position in favor of party autonomy. Many, if not most, of the provisions of the Law can be varied by agreement. Chapter II of the Law provides a "floor" of mandatory rules. The parties to a transaction cannot vary these rules by agreement.

Information[16] shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.[17] The reasons for denying legal effect to data messages are as varied as the number of legal systems which enact the Law.

Some courts deny legal effect to electronic documents because electronic documents are not considered a writing. In case of the United States, the Statute of Frauds[18] (and the related Statute of Wills[19]) is part of our legal heritage from England. The concepts behind it are included in

---

14. While the Guide to Enactment says Article 3 was inspired by Article 7 on the Vienna Sales Convention, it is common practice to insert such clauses in legislation drafted by the National Conference of Commissioners on Uniform State Laws. For example, Uniform Commercial Code Section 1-102 provides:

> (1) This Act shall be liberally construed and applied to promote its underlying purposes and policies.
>
> (2) Underlying purposes and policies of this Act are:
>
> (a) to simplify, clarify and modernize the law governing commercial transactions;
>
> (b) to permit the continued expansion of commercial practices through custom, usage and agreement of the parties;
>
> (c) to make uniform the law among the various jurisdictions.

The October 8, 1998 draft of the new Uniform Arbitration Act provides in Section 28 that: "In applying and construing the [Act], consideration must be given to the need to promote uniformity of the law with respect to its subject matter among States that enact it."

15. For subscription information, please contact UNCITRAL Secretariat, Vienna International Centre, P.O.Box 500, A-1400 Vienna, Austria; Telephone No. (011)(43 1) 21345-4060; Fax: (011)(43 1) 21345-5813; E-mail: uncitral@unov.un.or.at.

16. This term is not defined in the Law.

17. Law, *supra* note 7, art. 5.

18. 29 Charles II C. 3 (1677).

19. 32 Henry VII C. 1 (1540).

numerous pieces of legislation, ranging from the Uniform Commercial Code[20] to the Uniform Probate Code.[21]

The definition of a writing was not specified in the original Statute of Frauds or any subsequent enactment. It is very likely the original framers intended whatever medium a prudent businessman would use.[22] Over time, this would have ranged from stone tablets to clay tablets, papyrus, parchment, paper, microfilm, and electronic storage media. This means the concept of what constitutes a writing has been left to a case-by-case analysis by our judges.

Scholars have written on this topic. Some have argued data messages meet the requirements of the statute of frauds.[23] Others have advocated the concept of having a more traditional paper writing to validate subsequent electronic writings for the purposes of the Statute of Frauds.[24] These writings seem have gone unnoticed by most of the judiciary.

The Law mandates that every data message shall be deemed a writing as long as it is preserved in such a way that can be referred to in the future. The Law allows each state to exempt certain types of transactions from this rule. For example, deeds to transfer commercial real estate are arguably within the scope of the Law.[25] A state may elect to exclude deeds for commercial real estate because it has no facilities to record electronic deeds. While the general rule may be uniform, the exceptions will be based upon local concerns and conditions.

The next hurdle imposed by the Statute of Frauds is that the writing must be signed. When most people sign a document, they place a handwritten signature on a piece of paper. The reason they place a handwritten signature on the paper is to authenticate the contents of the writing. A signature is simply any mark[26] made with the present intent to authenticate a writing.[27] While a handwritten signature at the bottom of a

---

20. U.C.C. § 1-206, § 2-201, §2 A-201 and § 5-104 (1997).

21. Uniform Probate Code § 2-502(a)(1).

22. Houston Lowry, *Does Computer Stored Data Constitute a Writing for the Purposes of the Statute of Frauds and the Statute of Wills?*, 9 RUTGERS COMPUTER TECH L. J. 93, 99 (1982); *See,* Clason v. Bailey, 14 JOHNS. 484 (N.Y. 1817); Rabel, *The Statute of Frauds and Comparative Legal History*, 63 L.Q. REV. 174, 182 (1947); Comment, *Sufficiency of the Writing and Necessity of a Signature in the Statute of Frauds of the Uniform Commercial Code*, 4 U.S.F. L. REV. 177, 184 (1969).

23. *Does Computer Stored Data Constitute a Writing for the Purposes of the Statute of Frauds and the Statute of Wills?*, 9 RUTGERS COMPUTER & TECH. L.J. 93 (1982).

24. American Bar Association Electronic Data Messaging Task Force, *The Commercial Use of Commercial Data Interchange - Report and Model Trading Partner Agreement*, 45 BUS. LAW. 1645, 1680 (1990).

25. It is difficult to claim a will is within the scope of the Law. There are grey areas, such as trusts (which can be used for business purposes, such as a Massachusetts Business Trust).

26. Can include marks, such as an *X*. *See* U.C.C. § 1-201 comment 39 (1997).

27. U.C.C. § 1-201(39) (1997).

piece of paper may be presumed to show a certain intent, that presumption can be rebutted. The presumption may be overcome by testimony or other competent evidence.

A similar result occurs in the electronic world, even though there is no handwritten signature. An electronic signature must identify the signer and indicate the signer's approval of the information contained in the data message.[28]

The next issue is the reliability of the signature. Simply typing the author's name at the end of a data message carries virtually no indicia of reliability because anyone with a computer can do it. Taking the typed name in conjunction with the internet e-mail address on the data message adds slightly more reliability.[29] Signing a data message with public key cryptography system is even more reliable.[30] Future technologies may be even more secure.

The Law does not require absolute security. Forgers and forgeries still exist in a paper based world. Forgers and forgeries will continue to exist in an electronic world. The Law merely requires the method of signing to be appropriate for the circumstances.[31] For large but infrequent transactions, it makes good business sense to require a very secure signature. The risk of loss is great enough to justify the time and expense of using a secure signature.

When the transactions are small and frequent, a very secure signature is not necessary. The risk of loss on each transaction is small. It might not be possible to use a secure signature on each transaction due to time constraints. In very small transactions (such as ATM transactions), the signature may not be very secure at all.[32]

The parties are free to agree on the level of security necessary for their transaction.[33] This agreement is but one of the factors which must be evaluated to determine the reasonableness of the signature.[34] Other factors include:

1. The sophistication of the equipment used by each of the parties;
2. The nature of their trade activity;
3. The frequency at which commercial transactions take place between the parties;

---

28. Law, *supra* note 7, art. 7(1)(a).
29. Although an internet e-mail address can be forged, doing so is fairly difficult.
30. As the bit size of the key- pair increases, it becomes much harder to forge.
31. Law, *supra* note 7, art. 7(1)(b).
32. The signature may consist of only a four-digit number.
33. Law, *supra* note 7, arts. 4(1), 7(1)(b); Guide to Enactment, para. 60.
34. Guide to Enactment, para. 58.

4. The kind and size of the transaction;
5. The function of signature requirements in a given statutory and regulatory environment;
6. The capability of communication systems;
7. Compliance with authentication procedures set forth by intermediaries;
8. The range of authentication procedures made available by any intermediary;
9. Compliance with trade customs and practice;
10. The existence of insurance coverage mechanisms against unauthorized messages;
11. The importance and the value of the information contained in the data message;
12. The availability of alternative methods of identification and the cost of implementation;
13. The degree of acceptance or non-acceptance of the method of identification in the relevant industry or field both at the time the method was agreed upon and the time when the data message was communicated; and
14. Any other relevant factor.

The next problem that arises is the best evidence rule.[35] Simply put, this rule requires the original of a document to be put into evidence. The whereabouts of an original must be accounted for before a copy may be put into evidence. Even then, only a reliable copy may be put into evidence.

This creates problems in the computer context. The original of a data message is on the sender's computer.[36] A copy was made to read the data message from the hard drive into the computer's central processing unit. From there, another copy is placed into the computer's random access memory.

Once the decision is made to send the data message, another copy is made from the random access memory and put into the central processing unit. From there, another copy goes into a data bus to a modem. The data message may go through one, or more than one, electronic intermediaries[37]

35. *See* FED. R. EVID. 1002 and 1003.
36. And no one can see it without making a copy of it.
37. Law, *supra* note 7, art. 1(e).

to reach the other end. At the receiving end, a similar process happens to put the data message on the recipient's hard drive.[38]

So which is the original? The sender views the copy on his hard drive as the original. The recipient views the copy on his hard drive as the original. The copies in between may not be writings within the meaning of the Law because they are not accessible for future reference.[39] Any printout of the hard disk data message from either the sender or the recipient is still only a copy.

This is an interesting intellectual exercise, but it overlooks one important fact. All of the copies are identical in all meaningful ways. The purpose behind the best evidence rule is to make sure the copy is an accurate, reliable copy.

The Law recognizes this purpose. A data message is considered an original if it meets two tests.[40] First, there must be a reliable assurance the copy of the data message is accurate.[41] The fact that additions are made to the original data message, such as endorsements, certifications, and notarizations, does not change the nature of the data message as an original (the same as in a paper context).[42]

What constitutes a "reliable assurance" is not clear. There is no explanation in the Law's Guide to Enactment. Therefore, this will have to be developed on a case-by-case basis. Courts may turn to the factors used to evaluate the reliability of a signature by analogy.[43]

The second test requires that the information can be displayed on demand.[44] This is a corollary of the writing requirement.[45] The data message must be preserved sufficiently so it can be referred to in the future. Businesses keep records so they can operate. Such records are not merely kept for no purpose at all; they will be referred to in the future. A business will not allow a computer to operate without creating a sufficient audit trail to show what happened and why it happened.

If data messages are to be given true legal effect, they must be admissible into evidence. When computer records were new, courts required computer experts to testify about the underlying computer system as an evidentiary predicate.[46] A business person could testify how the

---

38. And even then, the data message cannot be seen without making one or more further copies of it.

39. Law, *supra* note 7, art. 6(1).

40. *Id.* art. 8(1).

41. *Id.* art. 8(1)(a).

42. *Id.*; Guide to enactment, para. 67.

43. Law, *supra* note 7, art. 8(1)(a); Guide to enactment, para. 58.

44. Law, *supra* note 7, art. 8(1)(b).

45. *Id.* art. 6(1).

46. American Oil v. Valenti, 179 Conn. 349 (1979), *compare* New England Savings Bank v. Bedford Realty Corp., 246 Conn. 594 (1998).

computer was used in the business once the reliability of the underlying computer system was established. Article 9 may very well eliminate the need for a computer expert to get computer documentation into evidence.

The court should no longer require a systematic analysis of how the underlying computer works. The data message should be allowed admission into evidence once a simple business record foundation is laid. Evidence of the reliability of the underlying computer system will only go to the weight of the evidence, not its admissibility.[47]

Evidence about the reliability of data message may be satisfied by the signing requirement instead of a description of the underlying computer system. For example, public key cryptography may prove reliability of a data message without reference to the underlying computer system through the signing process. In the future, there may be even more reliable ways to determine when a data message is altered.

The law often requires that information must be stored. Sometimes the method of storage is specified. Article 10 of the Law imposes three requirements to determine if a data message was properly stored.

First, the information in the data message must be accessible for future reference.[48] This is the same requirement used to determine if there is a writing.[49] It is similar to the requirement of a reliable assurance about the integrity of the information contained in a data message.[50] It boils down to a record must be of such a nature that it can reliably referred to when needed.

Second, the information must be retained in the form it was sent.[51] This means a data message cannot simply be split up into separate parts and stored separately. There must be a copy of the original data message preserved in such a way that any alterations will be evident.[52] In essence, there must be a complete audit trail. It is not sufficient to simply show what your computer did when it got the data message. You must show what data message your computer got in the first place.[53]

Third, certain information from the data message must be preserved.[54] While there is no requirement this information exist, the information must be preserved if it exists. This information includes an identification of the data message's origin, the date and time it was sent, the date and time it was received, and an identification of the data message's destination. Once

---

47. Law, *supra* note 7, art. 9(2).

48. *Id.* art. 10(1)(a).

49. *Id.* art. 6(1).

50. *Id.* art. 8(1)(a).

51. *Id.* art. 10(1)(b).

52. Compare this to the reliable assurance standard in Law, *supra* note 7, art. 8(1)(a).

53. As time goes on, court interpretation of this requirement will loosen.

54. Law, *supra* note 7, art. 10(1)(c).

again, all of this information is likely to be present in the commercial context.

The duty of storing a data message may be delegated to a third party.[55] The Law does not require the preservation of information whose sole purpose is to permit the data message to be sent or received (i.e.: internet headers).[56] Such information may be deleted before the data message is stored.

The Law goes on to clearly indicate that an offer and an acceptance can occur by data messages.[57] The casual reader may wonder why this provision is even necessary. The simple reason is electronic agents.

While there may be a human being at either end of a data message today, this will not always be true in the future. Eventually, one side will be a computer program.[58] Eventually, there may even be computer programs at both ends.

The fact that a program is at one end of an exchange instead of a person doesn't prevent a contract from being formed. For example, the author filled out an application for an on-line stock brokerage account. In due course, a data message was received by the author giving all of the details of the account, including the account number and password. At the end of the data message appeared a line to the effect the author should not reply to the e-mail because the sender was an electronic agent (computer program). Did the author expect he was going to deal with an electronic agent? No.

Should the fact the acceptance of the author's offer was sent by an electronic agent affect the contract between the author and the stock brokerage firm? It should not, particularly since one party (the author) did not know he was dealing with an electronic agent.[59] Perhaps the author was dealing with a person masquerading as a computer program. The expectations of the parties should be enforced, meaning the law should find that there was a contract formed by this exchange of data messages.

Article 12 governs a related issue. A statement of will or other notice given by a data message cannot be invalidated solely on the ground it was given by a data message.[60] This means that notices given pursuant to contract may be given in the form of a data message, then the data message is attributed to the originator.[61] This seems rather straight forward.

---

55. *Id.* art. 10(3).

56. Such as fax handshaking, fax training and the like.

57. Law, *supra* note 7, art. 11.

58. *Normalization: A Revolutionary Approach*, 20 JURIMETRICS J. 140 (1979).

59. Although this does raise interesting questions about proving contracts of adhesion.

60. Law, *supra* note 7, art. 12(1).

61. *Id.* art. 13(1).

If any agent with authority sends a data message, the originator of the data message is deemed to have sent it.[62] Although the Law does not discuss such common law concepts as actual authority, apparent authority and agency by estoppel, the concept of an agent acting for a principal is common enough in all legal cultures. Perhaps it is even universal as a general concept.

The next rule is an out growth of the electronic agent concept. An originator is bound by a data message sent by the originator's electronic agent.[63] An electronic agent is as much an agent as a human agent. This creates another corollary; an originator is responsible for the originator's electronic agent's errors (perhaps caused by programming errors). When human agent makes a mistake or acts beyond the wishes of the agent's principal, the principal is still bound. Likewise the principal is still bound by the actions of its electronic agent when the agent "malfunctions."

The problem arises when the data message was not truly sent by the originator. If the forger sends a data message using a procedure previously agreed between the originator and the addressee (such as a data message signed by the originator's private cryptography key, - which is actually verified by the originator's related public cryptography key), then the originator is bound by the data message even if the originator did not actually send the data message.

This is slightly different, although related, the concept of a signing in Article 7. While a signature is evaluated against the parties' agreement, it is also evaluated against fourteen other factors. In the attribution context, there is no background of fourteen factors. The parties' agreement is the sole factor.

This gives rise to the interesting question of what happens when a data message is not signed within the meaning of Article 7 but can be attributed to the originator under Article 13. This question must be resolved in light of local law. If local law requires a signature on this particular type of data message, then the fact it can be attributed to the originator is meaningless.

There is another type of data message, which will be attributed to the originator. If an ex-employee or ex-agent of the originator uses the knowledge he obtained from his relationship with the originator (ie: takes a copy of the originator's private cryptography key and uses it to authenticate data messages), then the originator is bound by the data message.[64] This gives a clear message to people who use electronic commerce: change your authentication procedures as employees leave. If you do not, they can still act on your behalf.

---

62. *Id.* art. 13(2)(a).

63. *Id.* art. 13(2)(b).

64. *Id.* art. 13(3)(6).

There are some things the originator can do to protect itself. If the originator requires an acknowledgment by the recipient of receipt[65] and notices a falsified data message, the originator can notify the addressee. Once the addressee receives the notice and has a reasonable time to act, *future* data messages cannot be attributed to the originator. It is important to note that such notices are *not* applied retroactively. Undoubtedly only the vigilant can take advantage of such procedures. In the case of transactions where the risk of loss is great, the Law will apply an incentive for everyone to be vigilant.

Sometimes the originator requires an acknowledgment by the recipient of the receipt of the data message by the recipient.[66] If the parties have not agreed to a particular method of acknowledgment, the data message can be acknowledged in either of two different methods.

The first method allows acknowledgment by any communication by the addressee, whether or not automated.[67] The acknowledgment could be the functional equivalent of a postal return receipt.[68] The acknowledgment could range from the mere acknowledgment of an unspecified data message to a communication that refers to the content of the original data message.

The second method allows acknowledgment by conduct.[69] If the parties have agreed to a particular form of conduct as an acknowledgment, the conduct must conform to the agreement. Otherwise, the conduct must be of such a nature to notify the originator of the data that it had been received. For example, shipping the goods indicates the data message containing the order was received.

If the originator wants to get an acknowledgment before the goods are actually shipped, the originator can make the original data message conditional upon the receipt of an acknowledgment.[70] Conditions may be attached to the acknowledgment.[71] For example, the originator may require an acknowledgment within a particular time.[72] Similarly, the originator may require the acknowledgment to be done a particular way. If the two elements are combined, an acknowledgment in a particular format is required within a particular time.

If the proper acknowledgment is not given in a timely fashion, the original data message is deemed never to have been sent. If no time period for the acknowledgment is specified, a court will likely imply the acknowledgment must be given within a reasonable period of time. The

---

65. Law, *supra* note 7, art. 14.
66. *Id.*
67. *Id.* art. 14(2)(a).
68. Guide to Enactment, para. 99.
69. Law, *supra* note 7, art. 14(2)(b).
70. *Id.* art. 14(c).
71. *Id.;* Guide to enactment, para. 95.
72. *Id.*

difficulty will be in determining what is reasonable under the circumstances.

What happens if the originator has not specified the original data message is conditioned upon the receipt of an acknowledgment and nothing happens?[73] The originator may send a data message to the recipient giving a reasonable time for the acknowledgment to be received.[74] Of course, the originator must give the recipient notice of the deadline.[75]

Article 15(5) creates a rebuttable presumption[76] that an acknowledgment of a data message implies the underlying data message was received. There is no presumption that the data message that was sent is the same as the data message that was received. The parties must still comply with the attribution procedure to verify the content of the data message.[77] If the acknowledgment indicates the underlying data message meets certain technical standards, it is presumed those standards have been met.[78] This seems to suggest a detailed acknowledgment will raise at least a presumption the underlying data message was in a particular format or possibly even validly signed by a recognized originator.

In commercial transactions, it is very important to determine when a data message was sent and when it was received. The Law has a number of rules relating to these issues. For example, a data message is deemed sent when it enters an information system outside of the originator's control.[79] Comparing this to the paper based postal system, the data message is deemed sent when it is placed in the postal box. This is in accord with existing commercial law in the United States.

A data message is deemed received when it enters the recipient's information system, regardless of when the data message is actually accessed.[80] This rule encourages recipients to check their electronic mailboxes frequently.

If the recipient of a data message specified the receiving computer system and the originator misdirected the data message, the data message is not deemed received until the recipient retrieves it from the information system.[81] This means companies will specify what computer or computer account must receive their data messages.

---

73. For example, a reasonable period of time may elapse (which depends upon the circumstances) or the time specified in the original data message may expire.

74. Law, *supra* note 7, art. 14(4)(a).

75. This is similar to other international convention promulgated by UNCITRAL. *See,* 1980 UNCITRAL Convention on the International Sales of Goods, arts. 47, 63; for an example.

76. *See generally supra* note 7; Guide to enactment, para. 97.

77. *See generally supra* note 7; Guide to enactment, para. 97, art. 13.

78. Law, *supra* note 7, art. 14(6).

79. *Id.* art. 15(1).

80. *Id.* at 15(1)(a)(b).

81. *Id.* at 15(2)(a)(ii).

Another question arises about where the data message is received or sent. An originator can send a data message from the office, the home or on the road. The recipient has no way to determine where the originator was physically when the data message was sent (a similar problem exists on the receiving end). The Law presumes the data message was sent from the originator's place of business.[82] If there is more than one place of business, the data message is deemed sent from the place of business with the closest relationship with the transaction.[83] If there is no underlying transaction, the data message is deemed to be sent from the originator's principal place of business. If the originator has no place of business, the data message is deemed to be sent from the originator's habitual residence.[84] This is similar to other international texts promulgated by UNCITRAL.[85] In many commercial cases, this rule will determine the applicable law for the underlying contract.

The balance of the Law governs the carriage of goods, including bills of lading.[86] Basically, the Law permits (but does not mandate) electronic bills of lading. It was anticipated when the Law was written that future projects relating to special cases of electronic commerce would be added here.

In summary, the Law is designed to promote, but not require, electronic commerce. This is done by removing traditional legal impediments to electronic commerce. A data message is not only a writing, but is also an original and can be signed. The law does not require any particular technology as long as the technology meets the policy objectives behind the law. There was nothing to be gained by restricting the Law to any particular technology.

As with any new law, the Law's success will depend on how judges interpret it and how they apply it. While a judge can justify any particular decision, the Law and the policies behind it will only work if the Law is sufficiently liberally construed to effectuate those policies.

---

82. *Id.* at (4).

83. Law, *supra* note 7, art. (4)(a).

84. *Id.* at (4)(b).

85. *See,* 1980 UNCITRAL Convention on Contracts for the International Sale of Goods, Article 10, for an example.

86. Law, *supra* note 7, art. 16, 17.

APPENDIX I

UNCITRAL Model Law on Electronic Commerce

[Original: Arabic, Chinese, English, French, Russian, Spanish]

Part one. Electronic commerce in general

Chapter I. General provisions

*Article 1. Sphere of application**

This Law** applies to any kind of information in the form of a data message used in the context*** of commercial**** activities.

* The Commission suggests the following text for States that might wish to limit the applicability of this Law to international data messages:
"This Law applies to a data message as defined in paragraph (1) of article 2 where the data message relates to international commerce."

** This Law does not override any rule of law intended for the protection of consumers.

*** The Commission suggests the following text for States that might wish to extend the applicability of this Law: "This Law applies to any kind of information in the form of a data message, except in the following situations: [...]."

**** The term "commercial" should be given a wide interpretation so as to cover matters arising from all relationships of a commercial nature, whether contractual or not. Relationships of a commercial nature include, but are not limited to, the following transactions: any trade transaction for the supply or exchange of goods or services; distribution agreement; commercial representation or agency; factoring; leasing; construction of works; consulting; engineering; licensing; investment; financing; banking; insurance; exploitation agreement or concession; joint venture and other forms of industrial or business cooperation; carriage of goods or passengers by air, sea, rail or road.

Article 2. Definitions

For the purposes of this Law:

(a) "Data message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy;

(b) "Electronic data interchange" (EDI) means the electronic transfer from computer to computer of information using an agreed standard to structure the information;

(c) "Originator" of a data message means a person by whom, or on whose behalf, the data message purports to have been sent or generated prior to storage, if any, but it does not include a person acting as an intermediary with respect to that data message;

(d) "Addressee" of a data message means a person who is intended by the originator to receive the data message, but does not include a person acting as an intermediary with respect to that data message;
(e) "Intermediary", with respect to a particular data message, means a person who, on behalf of another person, sends, receives or stores that data message or provides other services with respect to that data message;
(f) "Information system" means a system for generating, sending, receiving, storing or otherwise processing data messages.

Article 3. Interpretation

(1) In the interpretation of this Law, regard is to be had to its international origin and to the need to promote uniformity in its application and the observance of good faith.
(2) Questions concerning matters governed by this Law which are not expressly settled in it are to be settled in conformity with the general principles on which this Law is based.

Article 4. Variation by agreement

(1) As between parties involved in generating, sending, receiving, storing or otherwise processing data messages, and except as otherwise provided, the provisions of chapter III may be varied by agreement.
(2) Paragraph (1) does not affect any right that may exist to modify by agreement any rule of law referred to in chapter II.

Chapter II. Application of legal requirements to data messages

Article 5. Legal recognition of data messages

Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

Article 6. Writing

(1) Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.
(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing.
(3) The provisions of this article do not apply to the following: ...

Article 7. Signature

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:

(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and

(b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(3) The provisions of this article do not apply to the following: [...]

Article 8. Original

(1) Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:

(a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and

(b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being presented or retained in its original form.

(3) For the purposes of subparagraph (a) of paragraph (1):

(a) the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and

(b) the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

(4) The provisions of this article do not apply to the following: ...

Article 9. Admissibility and evidential weight of data messages

(1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:

(a) on the sole ground that it is a data message; or

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.

Article 10. Retention of data messages

(1) Where the law requires that certain documents, records or information be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied:

(a) the information contained therein is accessible so as to be usable for subsequent reference; and

(b) the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

(c) such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received.

(2) An obligation to retain documents, records or information in accordance with paragraph (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

(3) A person may satisfy the requirement referred to in paragraph (1) by using the services of any other person, provided that the conditions set forth in subparagraphs (a), (b) and (c) of paragraph (1) are met.

Chapter III. Communication of data messages

Article 11. Formation and validity of contracts

(1) In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.

(2) The provisions of this article do not apply to the following: ...

Article 12. Recognition by parties of data messages

(1) As between the originator and the addressee of a data message, a declaration of will or other statement shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

(2) The provisions of this article do not apply to the following: ...

Article 13. Attribution of data messages

(1) A data message is that of the originator if it was sent by the originator itself.

(2) As between the originator and the addressee, a data message is deemed to be that of the originator if it was sent:

(a) by a person who had the authority to act on behalf of the originator in respect of that data message; or

(b) by an information system programmed by, or on behalf of, the originator to operate automatically.

(3) As between the originator and the addressee, an addressee is entitled to regard a data message as being that of the originator, and to act on that assumption, if:

(a) in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or

(b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own.

(4) Paragraph (3) does not apply:

(a) as of the time when the addressee has both received notice from the originator that the data message is not that of the originator, and had reasonable time to act accordingly; or

(b) in a case within paragraph (3)(b), at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was not that of the originator.

(5) Where a data message is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the data message as received as being what the originator intended to send, and to act on that assumption. The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received.

(6) The addressee is entitled to regard each data message received as a separate data message and to act on that assumption, except to the extent that it duplicates another data message and the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was a duplicate.

Article 14. Acknowledgement of receipt

(1) Paragraphs (2) to (4) of this article apply where, on or before sending a data message, or by means of that data message, the originator has requested or has agreed with the addressee that receipt of the data message be acknowledged.

(2) Where the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by

(a) any communication by the addressee, automated or otherwise, or

(b) any conduct of the addressee, sufficient to indicate to the originator that the data message has been received.

(3) Where the originator has stated that the data message is conditional on receipt of the acknowledgement, the data message is treated as though it has never been sent, until the acknowledgement is received.
(4) Where the originator has not stated that the data message is conditional on receipt of the acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator:

(a) may give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and

(b) if the acknowledgement is not received within the time specified in subparagraph (a), may, upon notice to the addressee, treat the data message as though it had never been sent, or exercise any other rights it may have.

(5) Where the originator receives the addressee's acknowledgement of receipt, it is presumed that the related data message was received by the addressee. That presumption does not imply that the data message corresponds to the message received.
(6) Where the received acknowledgement states that the related data message met technical requirements, either agreed upon or set forth in applicable standards, it is presumed that those requirements have been met.
(7) Except in so far as it relates to the sending or receipt of the data message, this article is not intended to deal with the legal consequences that may flow either from that data message or from the acknowledgement of its receipt.

Article 15. Time and place of dispatch and receipt of data messages
(1) Unless otherwise agreed between the originator and the addressee, the dispatch of a data message occurs when it enters an information system outside the control of the originator or of the person who sent the data message on behalf of the originator.
(2) Unless otherwise agreed between the originator and the addressee, the time of receipt of a data message is determined as follows:

(a) if the addressee has designated an information system for the purpose of receiving data messages, receipt occurs:

(i) at the time when the data message enters the designated information system; or

(ii) if the data message is sent to an information system of the addressee that is not the designated information system, at the time when the data message is retrieved by the addressee;

(b) if the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee.

(3) Paragraph (2) applies notwithstanding that the place where the information system is located may be different from the place where the data message is deemed to be received under paragraph (4).

(4) Unless otherwise agreed between the originator and the addressee, a data message is deemed to be dispatched at the place where the originator has its place of business, and is deemed to be received at the place where the addressee has its place of business. For the purposes of this paragraph:

(a) if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or, where there is no underlying transaction, the principal place of business;

(b) if the originator or the addressee does not have a place of business, reference is to be made to its habitual residence.

(5) The provisions of this article do not apply to the following: ....

Part two. Electronic commerce in specific areas

Chapter I. Carriage of goods

Article 16. Actions related to contracts of carriage of goods

Without derogating from the provisions of part one of this Law, this chapter applies to any action in connection with, or in pursuance of, a contract of carriage of goods, including but not limited to:

(a) (i) furnishing the marks, number, quantity or weight of goods;

(ii) stating or declaring the nature or value of goods;

(iii) issuing a receipt for goods;

(iv) confirming that goods have been loaded;

(b) (i) notifying a person of terms and conditions of the contract;

(ii) giving instructions to a carrier;

(c) (i) claiming delivery of goods;

(ii) authorizing release of goods;

(iii) giving notice of loss of, or damage to, goods;

(d) giving any other notice or statement in connection with the performance of the contract;

(e) undertaking to deliver goods to a named person or a person authorized to claim delivery;

(f) granting, acquiring, renouncing, surrendering, transferring or negotiating rights in goods;

(g) acquiring or transferring rights and obligations under the contract.

Article 17. Transport documents

(1) Subject to paragraph (3), where the law requires that any action referred to in article 16 be carried out in writing or by using a paper document, that requirement is met if the action is carried out by using one or more data messages.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for failing either to carry out the action in writing or to use a paper document.

(3) If a right is to be granted to, or an obligation is to be acquired by, one person and no other person, and if the law requires that, in order to effect this, the right or obligation must be conveyed to that person by the transfer, or use of, a paper document, that requirement is met if the right or obligation is conveyed by using one or more data messages, provided that a reliable method is used to render such data message or messages unique.

(4) For the purposes of paragraph (3), the standard of reliability required shall be assessed in the light of the purpose for which the right or obligation was conveyed and in the light of all the circumstances, including any relevant agreement.

(5) Where one or more data messages are used to effect any action in subparagraphs (f) and (g) of article 16, no paper document used to effect any such action is valid unless the use of data messages has been terminated and replaced by the use of paper documents. A paper document issued in these circumstances shall contain a statement of such termination. The replacement of data messages by paper documents shall not affect the rights or obligations of the parties involved.

(6) If a rule of law is compulsorily applicable to a contract of carriage of goods which is in, or is evidenced by, a paper document, that rule shall not be inapplicable to such a contract of carriage of goods which is evidenced by one or more data messages by reason of the fact that the contract is evidenced by such data message or messages instead of by a paper document.

(7) The provisions of this article do not apply to the following: ....